VALORIZA

INTERNAL INFORMATION SYSTEM POLICY

(ETHICS CHANNEL)

SUMMARY SHEET AND CHANGE CONTROL

TITLE	**INTERNAL INFORMATION SYSTEM POLICY (ETHICS CHANNEL)**	
DESCRIPTION	This Policy outlines the management and processing of reports received through the Internal Information System (Ethics Channel), through which potential whistleblowers may disclose facts that constitute breaches of the Compliance Model.	
SCOPE	All entities belonging to Valoriza, considering their individual characteristics, including subsidiaries or majority-owned companies in which Valoriza exercises effective control. Members of administrative and executive bodies and employees of all entities listed above. Third parties, both individuals and legal entities, related to Valoriza, to the extent that the provisions of this Policy are applicable to them. In general, any person who wishes to report potential non-compliance and/or violations to the organization.	
AFFECTED DEPARTMENTS	All	
AUTHOR	Regulatory Compliance Unit	
RESPONSIBLE PARTIES	**RESPONSIBLE**	**FUNCTIONS**
	Regulatory Compliance Unit	Distribution, monitoring, and oversight of the Policy.
	Other departments	Ensure compliance with the principles set forth in this Policy.
APPROVED BY	Board of Directors	
REVIEW PERIOD	Annual	

Version Register:

Edition	Date	Responsible Party	Description of Changes	Approved by
V1	29/11/2023	Regulatory Compliance Unit	Initial Draft	Initial Draft
V2	06/02/2024	Regulatory Compliance Unit	Draft v2.	Draft v2.
V3	06/03/2024	Regulatory Compliance Unit	Content adaptation	Board of Directors
V4	20/03/2024	Regulatory Compliance Unit	Content adaptation	Board of Directors
V5	24/07/2025	Regulatory Compliance Unit	Content adaptation	Board of Directors

ÍNDICE

INTERNAL INFORMATION SYSTEM POLICY (ETHICS CHANNEL)

The Board of Directors of Valoriza Servicios Medioambientales, S.A. (hereinafter, "**Valoriza**"), within the framework of its general and non-delegable authority to define general policies and strategies, has approved this Policy of the Internal Information System (hereinafter, the "**Policy**").

This Policy forms part of the "Compliance Management System for Criminal Prevention, Anti-Corruption, and Competition Law Compliance of Valoriza" (hereinafter, the "**Compliance Management System**").

The Code of Ethics of Valoriza is the internal regulation that serves as the foundation for this Compliance Management System. This Policy is aligned with the values of integrity and transparency set forth in the Code of Ethics and represents an instrument for ensuring its effective enforcement.

Consequently, this Policy must be read and interpreted in conjunction with the Code of Ethics and the other policies of Valoriza that further develop it, including, among others, the Procedure for Managing the Internal Information System.

1. PURPOSE

This Policy sets out the guidelines for the management and handling of communications received through the Internal Information System (hereinafter, the "Ethics Channel"), through which potential informants may report facts that constitute breaches of the Compliance Management System.

The purpose of this Channel is to facilitate the efficient receipt and processing of communications concerning conduct that may constitute a violation of the legal framework, as well as the principles set out in the Code of Ethics and other key documents that make up the Compliance Management System.

The aim is to establish an agile, accessible, and flexible system, in accordance with the provisions of Law 2/2023, of 20 February, regulating the protection of individuals who report regulatory infringements and the fight against corruption, and in line with national and international standards and best practices in compliance and corporate governance.

The system distinguishes between ordinary channels and others considered alternative, in order to ensure that potential informants can report facts or conduct that may be considered irregular, in a confidential manner, without fear of retaliation or adverse consequences, and with full protection of their rights throughout the process.

This Policy, together with the Procedure for the Internal Information Channel and Management of Reports, aims to ensure professional, confidential, impartial handling and the highest level of protection during the entire process, thereby fostering a climate of trust among stakeholders.

2. SCOPE OF APPLICATION.

For the purposes of this Policy, any reference to "Valoriza" or "the Company" includes the entities listed within this scope of application.

This Policy applies to:

- All entities belonging to Valoriza, taking into account their specific characteristics. For the purposes of this document, Grupo Valoriza is deemed to include all subsidiaries or majority-owned companies in which Valoriza, either directly or indirectly—including Temporary Business Joint Ventures (UTEs)—exercises effective control, regardless of their geographic location.
- In those entities in which Valoriza holds a stake without effective control, it will promote the adoption of conduct and operational standards aligned with this Policy.
- Members of the administrative and executive bodies, as well as employees of all the aforementioned entities of Valoriza, regardless of their role or position, the legal nature of their relationship, or their geographic location.
- Third parties, whether natural or legal persons, with a relationship to Valoriza, in those aspects of this Policy that are applicable to them, and from whom behavior consistent with this Policy is expected.
- In general, any person who wishes to report to the organization the existence of potential breaches and/or violations.

In the case of activities carried out by Valoriza outside of Spain, this Policy shall be adapted to the most restrictive applicable local legislation, where appropriate.

For these purposes, Valoriza has regulatory compliance clauses to be included in all contracts signed with third parties, its subsidiaries, and Joint Ventures.

These clauses will bind the parties to their commitment not to contravene, directly or indirectly, the policies, procedures and protocols of the Compliance Management System, the legislation and regulations in force in the jurisdictions that are applicable and, especially and without limitation, the legislation (i) of a criminal nature, (ii) on anti-corruption, (iii) on defence of competition, (iv) on personal data protection, (v) on prevention of money laundering and the financing of terrorism, (vi) on trade sanctions and export administration and control or, in general, (vii) any other laws, statutes, regulations, standards, decrees, etc. that are applicable.

In addition, the parties are informed of the existence of the Ethical Channel as a way to report possible breaches of these values and behavioural guidelines, as well as to formulate possible queries in this regard.

3. GOVERNING PRINCIPLES OF THE CHANNEL.

The general principles governing the Channel must be respected and guaranteed by all members of the organisation, in order to provide informants with adequate protection against possible reprisals that they may suffer for the mere fact of bringing to the attention of the organisation facts that may constitute a violation of the legal system or internal rules.

The Channel shall be governed by the following principles:

3.1. Accessibility.

The Channel must be clear, public and easily accessible to employees and third parties who wish to communicate, as the ideal medium for the organisation to listen and talk to all members of the organisation or other stakeholder third parties.

3.2. Good faith.

The informant must act in good faith and must base the report on facts or indications from which it can reasonably be inferred that improper, illegal, criminal behaviour or conduct contrary to the principles and values of the organisation have been committed. Knowingly and deliberately reporting false information, thereby causing harm, may result in disciplinary action.

3.3. Confidentiality.

The protection of confidentiality in general shall be ensured at all times. The informant's identity will be treated as confidential Information and may not be disclosed or revealed without his/her consent (unless required by Courts).

3.4. Objectivity and impartiality.

Once a communication is received, impartiality will be guaranteed, as well as the right of privacy, to defence and the presumption of innocence of everyone who is covered by it.

3.5. Transparency.

The Channel is a tool of transparency that fosters the trust of the organisation's people.

3.6. Authority, independence and conflicts of interests.

The channel manager and the Regulatory Compliance Unit will act with complete autonomy and independence at all times. If any of the persons participating in the investigation is involved in the facts that are reported or considers that they may be affected by any type of conflict of interest, they must refrain from participating in the management and subsequent investigation.

3.7. Prohibition of reprisals.

It is guaranteed that the use of this channel will not be subject to any reprisal, direct or indirect, against those persons who, in good faith, have reported an alleged irregularity.

3.8. Exemption from contractual obligations.

The possibility of using this channel will not be restricted on the basis of contractual obligations, such as non-disclosure agreements, clauses relating to commercial or labour confidentiality when the reporting person makes the communication based on reasonable grounds to believe that it is necessary to inform the organisation of an action that breaches the regulations or is an omission thereof.

4. CONDUCTS THAT MUST BE REPORTED.

Information on infringements or breaches is interpreted broadly, i.e. facts may be reported that may give rise to reasonable suspicion, are actual or potential breaches that have occurred or are likely to occur.

By way of illustration, some of the possible topics to be reported are outlined below:

- Bribery and corruption;
- Conducts that undermine health and safety in the workplace;
- Conflicts of interest;
- Discrimination, sexual harassment and harassment in the workplace;
- Internal fraud;
- Cases of unfair competition;
- Breaches with regard to the defence of competition;
- Irregularities with regard to tax or accounting, or that undermine integrity in business and in financial records.
- Revealing information whose disclosure could affect the entity's interests.
- Acts that are harmful to the environment.

4.1. Guarantees of the informant.

The Channel has the necessary assurances to maintain the security of communications and confidentiality between the informant and the Regulatory Compliance Unit.

Those responsible for the management of the channel will be aware of the content of each of the communications and will treat them with due diligence, always keeping the identity of the informant with the utmost confidentiality when the communication is not anonymous.

Any kind of retaliation against those who use this channel in good faith is strictly prohibited. If it is confirmed that such persons have been subjected to any form of reprisal, stigmatisation or humiliation, the perpetrators of such reprisals shall be subject to investigation and, where appropriate, disciplinary action.

4.2. Guarantees of persons that may be implicated.

Persons allegedly involved in the events that are communicated through the channel may never be punished for a simple communication or notification; in any case, the veracity of the report needs to be verified and they must be given the opportunity to offer an explanation of the reported situation.

Those potentially involved will be informed by the Regulatory Compliance Unit as soon as possible and no later than one month after receipt of the report, of the alleged facts, the person responsible for processing the communication, the next stages of the investigation and their data protection rights.

Exceptionally, if there is a significant risk that notification to the alleged suspect will jeopardise the effectiveness of the investigation or collection of evidence, notification will not be made until the risk no longer applies.

The reasons for specifying the existence of such a risk shall be documented and sufficiently supported, and the maximum period of one month may be extended for a period not exceeding three months.

All information with regard to the person(s) possibly implicated will be treated with the utmost confidentiality.

5. ESSENTIAL PRINCIPLES OF THE REPORTING HANDLING PROCEDURE.

5.1. Guiding principles of the procedure.

Taking into account the possible criminal consequences of the facts that can be communicated through the channel, its management will be aligned with the guiding principles of legal proceedings:

- Documentation: regardless of the channel of entry, the investigation procedure must be duly documented in writing.
- Who drives the investigation: once a communication of facts that indicate a breach or infringement is received, the investigation will depend on the will of the organisation, thus preventing the informant from misusing the channel.
- Right of challenge: during the investigation, the accused must be allowed at all times to exercise his or her rights of defence.

However, in the event that judicial proceedings are initiated within the internal investigation, and taking into account the possibility of criminal proceedings, said principles will be conditioned to the obligations established in the Spanish Criminal Procedure Act, the Spanish Civil Procedure Act and to any other regulations that must order the judicial procedure.

5.2. Sending an acknowledgement of receipt of the communication to the informant.

Within seven calendar days of receipt of the communication, unless this may jeopardise the confidentiality of the communication or the communication has been made anonymously, an acknowledgement of receipt will be sent to the informant.

5.3. Communication with the informant.

If necessary, communication may be maintained with the informant (if the informant identifies him/herself) and additional information may be requested.

5.4. Determination of the maximum period for responding to the investigation actions.

The time limit for replying to the informant may not exceed three months from receipt of the communication or, if no acknowledgement of receipt has been sent to the informant, three months from the expiry of the seven-day period after the communication has been made, except in particularly complex cases requiring an extension of the period. in which case, it may be extended up to a maximum of three additional months.

5.5. Admission, rejection and transfer to other channels.

A communication may be inadmissible on the grounds that it is not relevant, that it is inadmissible or not related to the matters to be communicated through the channel, and therefore the following are grounds for inadmissibility:

a) When the facts as reported are not credible.

b) When they do not constitute an infringement of the legal system.

c) When the communication is unfounded.

d) When the information does not contain new and significant information from a previous communication that has already been concluded.

In this case, this will be communicated with a rationale to the informant and the communication will be shelved; additionally and if necessary, the informant may be redirected to the appropriate channel in the event that his/her information does have a place in other spheres of action.

In the event that the complaint is considered relevant, a communication will be sent to the informant confirming the opening of the case.

5.6. Referral to the Public Prosecutor's Office.

The information received shall be immediately forwarded to the Public Prosecutor's Office when the facts may constitute an offence.

5.7. Opening of the investigation case.

When it is determined that the facts are sufficient evidence to indicate a possible breach, the corresponding internal investigation file will be opened

The Regulatory Compliance Unit will in principle be in charge of carrying out the investigation, unless a situation of conflict of interest is detected, in which case the Board of Directors will be informed and will make the decision to appoint someone to head the investigation, which may be internal or external.

The Chief Investigator will open the corresponding case, which will include all the incidents that occur in the carrying out his/her duties; it shall be confidential and shall be governed by the provisions of the regulations on the Protection of Personal Data and implementing regulations.

In the event that the facts are considered to be of a certain seriousness and urgent reaction or containment measures are necessary, the Investigation Report will be forwarded to senior management so that they are aware of this information and, if appropriate, can take a decision regarding the proposed measures.

Likewise, a prior analysis of the evidence provided will be made available to the accused of the facts so that he/she can claim what he deems appropriate in his/her defence, unless at this first instance it is determined that the communication is not appropriate so as not to hinder the investigation or prevent the destruction of evidence.

5.8. The internal investigation.

The Regulatory Compliance Unit will ensure that the investigation has all the necessary resources, whether internal or external, and that for this purpose it has access to all the information and documentation, as well as the people who may be related to the case depending on the specific circumstances.

5.9. Conclusions and proposal of actions to be taken.

Once the internal investigation has been completed within the established deadlines, the Investigation Minutes and Resolution Minutes will be drawn up.

5.10. Follow-up of decisions taken.

After the completion of the investigation process and once the decisions deemed appropriate have been made, the Regulatory Compliance Unit will follow up and monitor to ensure that the decisions taken are duly carried out.

The purpose of this follow-up and monitoring is to verify that the measures adopted are implemented, thus contributing to the continuous improvement of the organisation's SGCP [Compliance Management Stem, in its initials in Spanish], and to reinforcing the culture of Compliance.

6. RESOLUTION OF QUERIES.

The channel may likewise be used as an internal sources for receiving queries and issues raised about the process of reporting irregularities or about the implementation of the internal policies or the fulfilment of the legal obligations that affect the organisation.

7. RETENTION OF COMMUNICATIONS.

All the information generated by the communications will be kept in the systems and with the security measures established within the framework of its data protection management system, during the retention periods that may be determined internally in application of the applicable principles on personal data protection or for the periods of which, in accordance with the law, liability could arise as a result of the actions investigated.

The personal data shall be retained within the scope of the channel for a maximum period of three months from the report. When this time has elapsed, if the data are necessary to continue the investigation of the facts, they may continue to be processed for the purpose of the investigation underway or, where applicable, from the conclusion of the disciplinary, official or judicial procedure that they have instigated.

Communications that have not been processed may only be recorded in anonymised form.

Once the investigation is concluded, the essential information may be held on file by the designated responsible party to ensure the traceability, compliance and effectiveness of the Compliance Management System.

8. EXTERNAL CHANNELS.

The relevant authorities are informed that there are external information channels.

Currently, we inform of the existence of the following external channels that may be of interest depending on the organisation's sector of activity and its scope of territorial action:

- ✓ Information channel on fraud or irregularities affecting EU funds of the National Anti-Fraud Coordination Service (SNCA, in its initials in Spanish). Ministry of Finance and Civil Service of the Government of Spain.
- ✓ European Anti-Fraud Office (OLAF).
- ✓ Andalusian Office Against Fraud and Corruption
- ✓ Anti-Fraud Office of Catalonia (OAC)
- ✓ Barcelona City Council's Ethics and Good Governance Mailbox;
- ✓ Madrid City Council Municipal Office against Fraud and Corruption.
- ✓ Office for the Prevention and Fight against Corruption in the Balearic Islands.

9. EFFECTIVE DATE, DISSEMINATION AND REVIEW

This document was approved by the Board of Directors of VALORIZA SERVICIOS MEDIOAMBIENTALES, S.A. on **24/07/2025**. Upon its entry into force, this Policy shall repeal any other internal regulation on the matter that may have been in effect until now.

This document shall be appropriately disseminated through the usual communication channels of the VALORIZA Group. Its content will be reviewed periodically, in accordance with the frequency established in the Organization’s documented information system, and on an extraordinary basis when relevant legal, organizational, or technical circumstances arise that justify its immediate adaptation.

Likewise, it will be regularly updated to reflect potential regulatory changes, structural modifications within the Group, or the incorporation of improvements resulting from reviews of the Criminal and Anti-Bribery Compliance Management System or the Compliance Management System. The current version of the document will be available at www.valorizasm.com.

In the event of a discrepancy between this procedure’s translation into other languages and its original version in Spanish, the Spanish version shall prevail.